TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

JOHANNES PARIKKA

LOHKOKETJUTEKNOLOGIA VERRATTUNA NYKYISEEN PANKKIJÄRJESTELMÄÄN

Kandidaatintyö

TIIVISTELMÄ

Johannes Parikka: Lohkoketjuteknologia verrattuna nykypäivän pankkijärjestelmään.
Kandidaatintyö, 27 sivua
Joulukuu 2017
Tuotantotalouden kandidaatin tutkinto-ohjelma
Pääaine: Tuotantotalous
Tarkastaja: professori Tuomas Korhonen

Avainsanat: lohkoketju, hajautettu järjestelmä, pankkitoiminta, elektroniset transaktiot, keskitetty järjestelmä, tietoturva

Rahoitusmarkkinat investoivat huomattavasti pääomaa lohkoketjuteknologiaan. Tästä herää kysymys, mitkä ovat nykypäivän pankkijärjestelmän ja lohkoketjuteknologian erot transaktiomenetelmässä. Kandidaatintyössä siis tarkastellaan pankkien markkina-asemaa sekä niiden elektronista transaktiomenetelmää. Tämän jälkeen esitellään lohkoketjuteknologian mahdollistama transaktiomenetelmä. Molempien transaktiomenetelmien rakenne ja toimintotavat analysoidaan yksityiskohtaisesti omissa luvuissaan ja niitä vertaillaan rinnakkain tulososiossa.

Kandidaatintyö toteutettiin kirjallisuuskatsauksena aikaisempaa tieteellistä lähdemateriaalia lohkoketjuteknologiasta sekä pankkijärjestelmästä hyödyntäen. Tutkimuksessa siis yhdistettiin pankkijärjestelmää sekä lohkoketjua tutkivia tieteellisiä julkaisuja ja analysoitiin niitä yhdessä. Kerätyn lähdemateriaalin pohjalta muodostettiin käsitys järjestelmien vahvuuksista ja heikkouksista. Työssä myös tarkasteltiin lohkoketjun nykypäivän käyttöastetta todentaen teknologisen kilpailun rahoitusalalla.

Työ kulminoituu järjestelmien vertailukriteereihin, jotka on muodostettu tieteellisen lähdemateriaalin perusteella. Kirjallisuuskatsauksesta selviää, että lohkoketjuteknologia suoriutuu paremmin transaktioiden verifioimisnopeudessa, käyttäjän tietoturvassa, transaktion kustannuksissa sekä kirjanpidossa. Toisaalta nykyinen pankkijärjestelmä suoriutuu paremmin asiakkaan suojaamisessa, skaalautuvuudessa, transaktion riitauttamisessa ja energiatehokkuudessa. Teknologiakeskeinen kilpaileminen rahoitusmarkkinoilla vaatii uusia innovaatioita, kuten lohkoketjuteknologian.

ABSTRACT

Johannes Parikka: Blockchain technology comparison with current banking system
Tampere University of Technology
Bachelor of Science Thesis, 27 pages
December 2017
Bachelor's Degree Programme in Industrial Engineering and Management
Major: Industrial management
Examiner: Tuomas Korhonen

Keywords: blockchain, decentralized system, banking system, electronic transactions, centralized system, cyber security

The financial market is investing a lot of capital in blockchain technology. This raises the research question, what are the key differences between current banking system and blockchain technology. The Bachelor's thesis, therefore examines banks' market position and their electronic transaction method. This is followed by the blockchain's transaction method. The structure and approaches of the both transaction methods are analyzed in detail in their own chapters and then compared in the result section.

The Bachelor's thesis was done as a literature review from earlier scientific source material dealing with blockchain and current banking system. This study therefore combines the current analysis of the banking system and blockchain technology. The scientific resources are analyzed together. The strengths and the weaknesses of the systems are analyzed with the collected source material. The Bachelor's degree also examines the current utilization of blockchain by verifying technological competition in the financial sector.

This thesis culminates in the benchmarking the different systems based on the scientific source material. As a result of the literature review, it is clear that the blockchain is better performing transaction verification speed, user security, transaction costs, and accounting. On the other hand, the current banking system performs better in customer protection, scalability, transaction disputes and energy efficiency. Technology-centric competition in financial markets requires new innovations, such as blockchain.

ALKUSANAT

Tämän kandidaatintyön aiheena on lohkoketjuteknologia verrattuna nykyiseen pankkitoimintaan. Aihepiirin valitseminen kandidaatintutkielmaan oli harkittu valinta, mutta itse tutkimuskysymyksen valitseminen muodostui haasteelliseksi. Lohkoketju on uusi teknologia eikä sitä ole tutkittu vielä paljoa. Täten halusin haastaa itseni oppimaan aivan uutta. Tutkimuskysymykseni muodostui lopulta tarkastelemaan nykyisen pankkitoiminnan järjestelmää verrattuna lohkoketjuteknologian mahdollistamaan järjestelmään. Työni aihe on omasta mielestäni hyvin ajankohtainen. Työssä siis selvitetään, millä vertailukriteereillä lohkoketjuteknologia suoriutuu paremmin kuin nykyinen järjestelmä. Aihe muodostui todella haastavaksi lähdemateriaalin niukkuudesta ja käsiteltävien järjestelmien monimutkaisuudesta. Tästä huolimatta olen itse hyvin tyytyväinen työhön ja kuinka paljon olen oppinut sen aikana.

Haluan kiittää Tuomas Korhosta ja Juho Kanniaista kandidaatintyöni ohjauksesta sekä rakentavasta palautteesta. Haluan myös kiittää opiskelukavereitani hyvistä vinkeistä, mielenkiinnosta työtäni kohtaan sekä yleisestä tsemppaamisesta.

Tampereella, 9.12.2017

Johannes Parikka

SISÄLLYSLUETTELO

KUVALUETTELO

TAULUKKOLUETTELO

LYHENTEET JA MERKINNÄT

P2P	Person to person
TTY	Tampereen teknillinen yliopisto

1. JOHDANTO

Lohkoketjun mahdollistama kaupankäynti on kasvanut kryptovaluuttojen suosion sekä niiden eksponentiaalisen arvonnousun kautta. Lohkoketjun ympärille syntyy uusia yrityksiä todella nopeasti ja uudet, lohkoketjuihin liittyvät projektit keräävät rahoituksensa todella nopeasti. On hyvin todennäköistä, että lohkoketjulla tulee olemaan suuri vaikutus finanssi- sekä muihin teollisuusaloihin (Fanning & Centers 2016).

Ennen lohkoketjun keksimistä tutkijat Haber ja Stornetta olivat jo tuoneet datan peräkkäisen arkistoinnin rakenteen esille vuonna 1991. He kutsuivat tätä nimellä ”Time-stamping”. Tämä arkistointimenetelmä luotiin digitaalisille asiakirjoille omaisuuden hallussapidon selkeyttämiseksi. (Yermack 2017) Lohkoketjun data arkistoidaan samalla periaatteella ja se tukeutuu juuri Haberin ja Stornettan luomaan konseptiin.

Lohkoketjuteknologia sai alkunsa 3.1.2009, kun nimimerkillä ”Satoshi Nakamoto” esiintyvä henkilö esitteli aikaansaannoksensa P2Pfoundation-nimisellä nettisivulla (Yermack 2017). Nakamoto esitteli julkaisussaan ensimmäisen toimivan kryptovaluutan, Bitcoinin, ja loi samalla ensimmäisen lohkon nykyiseen lohkoketjuun. Finanssikriisi vuosina 2007-2008 motivoi Nakamotoa luomaan transaktiojärjestelmän, jossa valtion vaikutus on suljettu pois (Fanning & Centers 2016).

Fanning & Centers (2016) mukaan Satoshin luoma lohkoketju oli avoimen lähdekoodin ohjelmisto. Tämä mahdollisti Bitcoinin syntymisen sekä lohkoketjun yleistymisen aiheesta kiinnostuneiden ohjelmoijien keskuudessa. Kaupallisesta näkökulmasta lohkoketju voidaan määritellä alustaksi, jossa käyttäjät voivat vaihtaa pääomaa transaktioilla ilman luotetun kolmannen osapuolen, tässä tapauksessa esimerkiksi pankin tarvetta. Lohkoketjun rakenne voidaankin hajauttaa niin, ettei mikään yksittäinen taho ole pääsääntöisesti vastuussa koko lohkoketjusta ja sen sisältämistä transaktioista (Bashir 2017, s.17). Järjestelmä siis jakaa vastuun käyttäjien kesken.

Lohkoketju koostuu datajoukoista, jotka muodostuvat taas datapaketeista. Nämä datapaketit ovat järjestetty ketjuksi. Lohkot ovat siis datapaketteja, jotka sisältävät useita transaktioita. Ketjua laajennetaan lisälohkoilla uusien transaktioiden tapahtuessa, ja näin ollen ketju sisältää koko tapahtumahistorian. Kukin uusi lohko sisältää aikaisempien lohkojen tapahtumahistoriat. Kasvava lohkoketjujen verkko pitää sisällään siis kaiken siihenastisen tapahtumahistorian lukuisia kertoja eri lohkoissa. Tämän ominaisuuden takia petokset pystytään ehkäisemään ja jäljittämään tehokkaasti. Kun jokin lohko väittää transaktion tapahtuneen eri tavalla, se tarkistetaan muiden lohkojen historiasta. Kun

suurin osa lohkoista on päätynyt eri tulokseen, vääristyneen lohkon tiedot mitätöidään. (Nofer et al. 2017)

Rahoitusalan katsotaan olevan lohkoketjun ensisijainen käyttäjä. Lohkoketjujen kasvava suosio ei ainoastaan johdu sen tunnetuimmasta sovelluksesta kryptovaluutta Bitcoinista, vaan kasvua syntyy myös rahoitusalalla vallitsevasta tehottomuus- ja kustannusongelmasta. (Nofer et al. 2017) Rahoitusalan suurin taho, Bank of America Merrill Lynch -korporaatio on aloittanut lohkoketjuteknologian implementoinnin omaan kaupankäyntiinsä ja liiketoimintaansa. Implementoinnilla pyritään hyödyntämään lohkoketjun mahdollistamaa nopeampaa, turvallisempaa ja läpinäkyvämpää transaktioita. (Zack Equity Research 2016)

1.1 Metodologinen kuvaus ja tavoite

Kandidaatintyötä varten tiedonhankinnassa käytetään TTY:n tarjoamia laajoja tietokantoja. Työssä hyödynnetään Google Scholar –hakukonetta sekä Web of science, Andor ja Scopus –tietokantoja. Näin varmistetaan, että kandidaatintyössä käytettävä lähdeaineisto täyttää tieteellisen tutkimuksen kriteerit, joita ovat objektiivisuus, luotettavuus ja toistettavuus (Nokelainen 2011).

Lohkoketju tutkimusaiheena on hyvin nuori, mikä tekee tiedonhankinnasta haasteellista. Tietoa haetaan pääsääntöisesti Google Scholar -hakukoneesta professori Juho Kanniaisen suosituksien mukaan. Tiedonhaku aloitettiin hakusanoilla ”Blockchain”,”Blockchain finance” ja ”cryptocurrencies”. Toiseen lukuun tiedonhaku aloitettiin hakusanoilla ”Banking”, ”Finance” ja ”History of finance”. Hakutuloksista avautuneista tieteellisistä julkaisuista tarkasteltiin uusia hakusanoja, joilla tarkennettiin kyseisen käsitteen määrittelyä sekä laajennettiin tutkimuskysymyksen tarkastelemaa näkökantaa.

Toisessa luvussa käytetyt lähteet ovat rahoitusalaa tutkivia tieteellisiä artikkeleita sekä lohkoketjuteknologiaa tarkastelevia tieteellisiä lähteitä. Osiossa on myös käytetty Bitcoinin white paperia. Toisen luvun lähdemateriaalista osa on vanhempia tieteellisiä artikkeleita ja osa hyvin uusia julkaisuja.

Kolmannessa sekä neljännessä luvussa lähteet painottuvat lohkoketjuteknologiaa sekä kryptovaluuttoja analysoiviin tieteellisiin julkaisuihin. Luvuissa on myös käytetty Bitcoinin white paperia. Työssä käytetyissä useissa lohkoketjua tarkastelevissa tieteellisissä julkaisuissa on myös tarkasteltu nykypäivän pankkijärjestelmää.

Luotettavien lähteiden löytäminen oli kandidaatintyössä haasteellisinta. Työssä on pyritty hakemaan ja hyödyntämään vain tieteellisiä julkaisuja tunnetuilta tutkijoilta, joihin on viitattu useita kertoja. Lähteitä on tarkasteltu Julkaisufoorumi-nimisen tietokannan kautta lähteen korkean laadun ja tiedon validiuden varmistamiseksi.

Kandidaatintyö on rajattu vertailemaan nykypäivän pankkijärjestelmän hyödyntävää transaktiomenetelmää ja lohkoketjuteknologian mahdollistamaa transaktiomenetelmää sekä lohkoketjuteknologian nykypäivän käyttöastetta

Tässä kandidaatintyössä ensin määritellään syy luotetun kolmannen osapuolen olemassaoloon markkinoilla. Tutkimus tarkastelee, miten pankkien elektroniset transaktiot tapahtuvat. Lisäksi työ tarkastelee kolmannen luotetun osapuolen tietojärjestelmärakennetta. Työ käsittelee myös lohkoketjun tarjoamaa transaktiomallia, lohkoketjun rakennetta ja lohkoketjun osien toimintaa. Tämän kandidaatintyön tavoitteena on vertailla edellä mainittujen transaktiomenetelmien toimintatapoja sekä niiden heikkouksia ja vahvuuksia. Työ tarkastelee myös lohkoketjuteknologian nykypäivän käyttöastetta.

1.2 Työn eteneminen

Kandidaatintyö on jaettu johdannon jälkeen kolmeen erilliseen osaan. Ensimmäinen osa tarkastelee, miksi ja miten pankkijärjestelmä on syntynyt. Osio käy läpi pankkijärjestelmän historiaa ja tarkastelee pankin rakennetta ja sen toimintaa. Osio paneutuu elektronisien transaktioiden toimintaan ja tarkastelee, miten pääoman siirtäminen Internetin välityksellä toimii. Osio tarkastelee myös tietoverkkojen rakenteita. Osio käsittelee, miten tietoverkkojen rakenteet ja pääoman siirtäminen verkossa liittyvät toisiinsa.

Toinen osa tarkastelee, millaisista osakokonaisuuksista lohkoketjuteknologia muodostuu ja miten alusta toimii. Lohkoketjua tarkastellaan monesta suunnasta ja paneudutaan varsinkin sen rakenteeseen ja toimintatapoihin. Osio käy lohkoketjun toimintatapaa yksityiskohtaisesti läpi. Merkittäviä osakokonaisuuksia ovat tietoturvallisuus sekä lohkoketjun hajautunut rakenne. Toinen osio myös esittelee kryptovaluuttoja, jotka pohjautuvat lohkoketjuteknologiaan.

Tulososio eli kolmas osio aluksi vertailee lohkoketjuteknologian ja pankkijärjestelmän eroavaisuuksia. Vertailukohteina ovat esimerkiksi järjestelmien rakenteet, luotettavuus ja transaktion verifiointi nopeus. Vastakkainasettelu paneutuu tarkastelemaan, mitä eroavaisuuksia transaktioiden toimintatavassa on ja miten tämä saattaa vaikuttaa finanssialaan. Tulososio tarkastelee myös teknologian käyttöastetta tällä hetkellä.

Neljäs luku eli yhteenveto tarkastelee sekä koostaa tutkimuksen ydinhuomiot kuten vertailtavien järjestelmien eroavaisuudet. Kerrataan nykypäivän käyttöaste sekä pohditaan rahoitusmarkkinoilla vallitsevaa teknologiakeskittymää ja lohkoketjuteknologian vaikusta rahoitusmarkkinoihin.

2. NYKYINEN JÄRJESTELMÄ

Tässä luvussa esitellään pankki- ja rahoitusalan toimintaa. Aluksi määritellään syy pankin tai muun luotetun kolmannen osapuolen olemassaoloon markkinoilla. Tässä kappaleessa tarkastellaan pankin asemaa markkinoilla ja pankin ydinosaamista. Tämän jälkeen siirrytään tarkastelemaan, miten pankkien elektroniset transaktiot toimivat ja mistä ne koostuvat. Samalla osiossa esitellään pankkien tietojärjestelmien rakenne sekä miten transaktiodata arkistoidaan. Osiossa tarkastellaan myös transaktiojärjestelmän vahvuuksia, epäkohtia ja heikkouksia.

2.1 Pankin olemassaolo

Pankki- ja rahoitusala sekä maksupalvelut ovat vanhimpien toimialojen joukossa. Nämä kaupalliset palvelut ovat varhaisemmalta ajalta kuin nykyaikainen kapitalismi ja ovat olleet olemassa jo ennen nykyaikaisia hallituksia. (Ferguson & Myers 2008, s. 41) Pankkien funktiot ja palvelut ovat monille tuttuja. Tasca et al. (2016) määrittelevät pankin funktioiksi pääoman tuotannon ja liikkeen. Tämä tarkoittaa esimerkiksi säästöjä ja sijoituksia sekä pankin myöntämiä lainoja. Myös maksujärjestelmän toiminta kuuluu pankin funktioihin (Tasca et al. 2016). Tämä tarkoittaa esimerkiksi pääoman siirtoja.

Coasen (1937), joka on luonut transaktiokustannustaloustieteen pohjan, esittelee pankkien olemassa olon juuri markkinoilla vallitsevien transaktiokustannusten perusteella. Henkilön, jolla on pääoman ylijäämää, osallistuminen rahoitusmarkkinoille olisi useasti kohtuuttoman kallista ja työlästä transaktiokustannusten takia. Transaktiokustannuksiin sisältyisi pääoman lainaajan etsiminen, sopimuksen laatiminen ja allekirjoittaminen, transaktion sekä sopimuksen valvominen. Tämä kaikki vaatisi valtavia määriä pääomaa, aikaa ja asiantuntemusta. Ylimääräisen pääoman omistaja uhraisi myös omaa likviditeettiään prosessiin. Tämä sama ongelma esiintyisi myös lainanottajalla, joka joutuisi itse löytämään potentiaalisen toimittajan vaatimillaan lainan ehdoilla. Esimerkiksi luotettavien osapuolten löytäminen transaktion molemmille puolille, sopivan takaisinmaksuajan ja koron asettaminen lainalle voi muodostua yllättävän haasteelliseksi. Ilman pankkeja, monet näistä pääomansiirroista eivät olisi ikinä toteutuneet. (Tasca et al. 2016) Toisin sanoen pankin lisäksi pääoman tarjoaja sekä lainaaja hyötyvät kyseisestä pankin tarjoamasta prosessista.

Yhteenvetona pankit toimivat luotettuna kolmantena osapuolena toimien välittäjänä eri osapuolten välillä. Välittäjänä toimiminen koostuu merkittävistä kuluista, kuten fyysisistä-, informaatio- sekä koordinointikustannuksista. (Dow & Earl 1982, s.140) Pankit siis sovittavat yhteen rahoitusomaisuuden tarjontaa sekä kysyntää

kustannustehokkaasti niin, että yksityinen henkilö ei voi kilpailla pankkien kustannustehokkuuden kanssa.

2.2 Elektroninen kaupankäynti

Nykypäivänä pankit toimivat organisaatioina, jotka palvelevat kaksipuolista markkinaa. Pankit sovittavat yhteen niitä, jolla on pääoman tarjontaa (säästäjät), sekä niitä, joilla on kysyntää pääomalle (lainaajat) (Rochet & Tirole 2003). Pankit siis toimivat välittäjänä edellä mainittujen säästäjien ja lainaajien välissä. Kaupankäynti nykypäivänä on siirtynyt suurimmalta osin fyysisistä transaktioista ja paperisesta kirjanpidosta Internetin välityksellä toimivaan elektroniseen kaupankäyntiin sekä digitaalisiin tietokantoihin. (Pinna & Ruttenberg 2016)

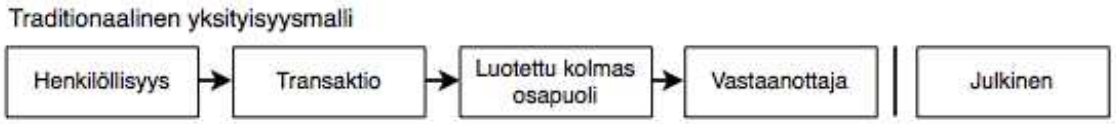
Pankkiorganisaatioissa on laajalti käytössä tietoverkkojen keskitetty malli (Pinna & Ruttenberg 2016), koska tämä malli on tehokkain tietorakenteiden luomiseen, julkaisemiseen sekä valvomiseen. Keskitetty järjestelmä minimoi kopioimista, esittää selkeän hierarkian järjestelmän sisällä sekä voi ratkaista tehokkaasti kiistoja. Keskitetyn mallin vahvuudet voivat myös esiintyä heikkouksina, sillä nämä samaiset keskitetyn mallin vahvuudet mahdollistavat järjestelmän väärinkäytön. Esimerkiksi talousjärjestelmissä keskitetyn mallin vahvuudet mahdollistavat inflaation, korruption ja välistävedon. Keskitetyn järjestelmän kasvaessa väärinkäytön riskit sekä järjestelmän ylläpitokustannukset kasvavat. (Fanning & Centers 2016)

Rahoitusmarkkinoiden yhteisen niin sanotun ”kultaisen tilikirjan” ylläpitäminen vaatii kommunikointia eri rahoitusalan organisaatioiden välillä. Näin toimialan infrastruktuurista vastaava hallintajärjestelmä ylläpitää tilikirjaa instituutioiden välisestä transaktioliikenteestä ja samalla eri pankkiorganisaatiot päivittävät omaa tietokantaansa. Rahoitusmarkkinoiden tietoliikenne jakautuu moniin erillisiin keskitettyihin tietokantoihin, jolloin transaktiotietojen jakaminen on tärkeää yhteisen tilikirjan ylläpitämiseen. Toisin sanoen transaktioiden tai muun päivityksen tapahtuessa muutos vahvistetaan rahoitusmarkkinan hallintajärjestelmän kautta. (Pinna & Ruttenberg 2016)

Meijerin (2016) mukaan elektronisessa kaupankäynnissä omistusoikeuden yhdistäminen anonyymiin omistajaan on mahdollista. Kuitenkin ainoastaan luotettu kolmas osapuoli voi muodostaa transaktion ostajan sekä myyjän välille ja vahvistaa omistajuuden. Toisin sanoen internetin välityksellä henkilöt eivät voi vaihtaa omaisuutta tai tuotteen omistajaa ilman luotettua kolmatta osapuolta.

Traditionaalisessa yksityisyysmallissa, jota pankit käyttävät, transaktion tiedot rajoitetaan kaupan osapuolien ja luotetun kolmannen osapuolen välille (Nakamoto 2008). Tiedot rajoitetaan julkisuudesta palomuurilla, mitä pystyviiva kuvassa 1 esittää. Pankkien

järjestel-missä tilikirjat säilötään siis pankin yksityiseen tietokantaan, arkistokaappiin tai kirjastoon, jota ei pääse ulkopuolelta tarkastelemaan. (Malinova & Park 2016) Näin kaikki transaktiotiedot pysyvät pois julkisuudesta luotettujen kolmansien osapuolien keskitetyillä tietojärjestelmillä. Tämä turvaa transaktiotietojen vuotamisen vääriin käsiin ja suojelee asiakkaiden yksityisyyttä. Kuitenkin tietojärjestelmän haltija pystyy havaitsemaan transaktion tiedot, kuten käytetyn rahasumman ja ostettavan tuotteen/palvelun, sekä yhdistämään tiedot ostajaan (Abrazhevich et al. 2001).



Kuva 1. *Traditionaalinen yksityisyysmalli, mukailtu lähteestä (Nakamoto 2008, s.6)*

2.3 Nykypäivän pankkitoiminnan transaktiot

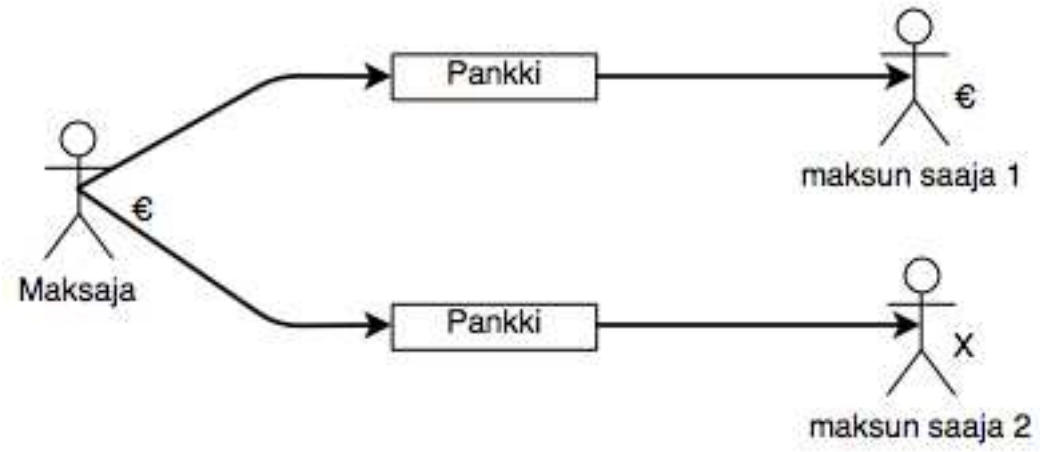
Kaupankäynti Internetissä on siirtynyt lähes yksinomaan rahoituslaitoksille, jotka tarjoavat rahansiirtopalveluita (Nakamoto 2008; Abrazhevich et al. 2001; Salem et al. 2003). Rahansiirrot toimivat pääasiassa halutulla tavalla, mutta transaktiot kärsivät silti monista ongelmista ja pohjautuvat luottamukseen. (Fanning & Centers 2016; Nakamoto 2008) Luottamus on peruselementti, joka mahdollistaa rahan vaihdon (Salem et al. 2003). Varsinkin Internetin välityksellä tehtävissä transaktioissa luottamus on yksi tärkeimmistä aspekteista (Knights et al. 2001). Kyseisessä transaktiossa transaktion osapuolet luovuttavat resurssejaan luotetulle kolmannelle osapuolelle, joka toimii oman etunsa mukaan, transaktion osapuolien edun mukaan tai kaikkien osapuolien eduksi (Jones et al. 2000).

Kaupankäynnissä käyttäjät luottavat, että transaktiot toimivat odotetulla tavalla. Samalla käyttäjät luottavat yllä esiteltyyn transaktiomenetelmään ja siihen, ettei luotettu kolmasosapuoli käytä asiakkaiden annettuja tietoja väärin. (Abrazhevich et al. 2001) Finanssi-instituutiot ovat muodostuneet kaupankäynnin turvaajiksi. He ovat saaneet aikaan niin sanotun ”instituutionaalisen luottamuksen” kuluttajien ja yritysten keskuudessa. Jos myyjän ja asiakkaan välisessä kaupassa loukataan luottamusta, transaktion takaaja, eli pankki tekee aloitteen asian ratkaisemiseksi. Näin epärehellisen osapuolen toiminta ei riko luotetun kolmannen osapuolen rakentamaa luottamusta. (Salam et al. 2003) Myös muilla tahoilla, kuten verkkokaupoilla, täytyy olla luottamus käytettävään maksujärjestelmään (Abrazhevich et al. 2001).

Täysin varmat eli peruuttamattomat transaktiot eivät siis ole mahdollisia maksun riitautusmahdollisuuden takia. Transaktioiden sovitteluista koituvat kustannukset näkyvät rahan siirroissa transaktiokustannuksina. Kyseiset kustannukset estävät pienien rahallisten summien siirtämisen, eli niin sanotut mikrotransaktiot kokonaan. (Nakamoto

2008; Abrazhevich et al. 2001; O'Mahony et al. 2001) Transaktiossa toimivien osapuolien täytyy siis ensiksi investoida resurssejaan jo ennen pääoman siirron tapahtumista. Usein riskiä alennetaan lakimääreisillä sopimuksilla, mutta juuri mikrotransaktioita tehdessä sopimuksetkaan eivät auta. (Coleman 1990, ss. 300-302) Salem et al. (2003) mukaan monia pieniä transaktioita ei kannata tehdä Internetin ylityksellä niiden suhteellisen suurien transaktiokustannusten takia.

Riitauttamisen vaara internetin välityksellä suoritetuista transaktioista vaatii esimerkiksi yrityksiä keräämään suuret määrät ylimääräistä tietoa asiakkaistaan edellä mainitun luottamuksen saavuttamiseksi. Internetin välityksellä tehdyissä transaktioissa petoksia pidetään väistämättöminä. Toisin sanoen tietty prosenttiosuus petoksista annetaan tapahtua, koska kaikkien petosten selvittäminen veisi liikaa resursseja. Yleisin tapa suorittaa petos on käyttää sama raha monta kertaa. (Nakamoto 2008) Tämä samainen ongelma tunnetaan tietojenkäsittelyopissa myös Byzantinin kenraalin ongelmana (Dourado & Brito 2014).

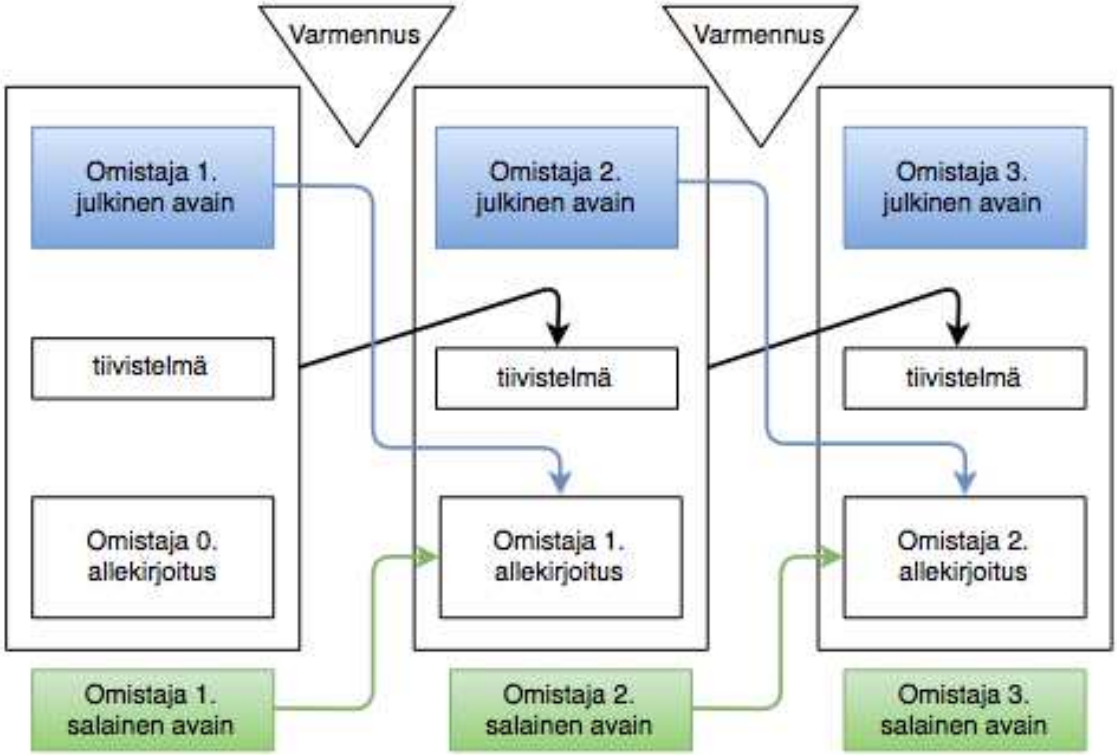


Kuva 2. . *Rahan moninkertainen käyttö*

Kuva 2 esittää Byzantinin kenraalin ongelmaa, eli rahan moninkertaista käyttöä, jossa sama raha käytetään tässä tapauksessa kaksi kertaa. Ainoastaan toinen maksun saajista saa rahan. Kuvassa 2 vasemmalla oleva maksaja tekee Internetin välityksellä kaksi saman suuruista transaktiota omistamallaan elektronisella kolikolla. Kolikon moninkertaista käyttöä ei huomata maksujen hyväksynnässä, jolloin sama elektroninen kolikko lähetetään molemmille maksun saajille. Kuvan keskellä oleva pankki huomaa kolikon monen kertaisen käytön ja estää sen. Näin ainoastaan maksun saaja 1 vastaanottaa maksajan rahan.

Nykyisessä rahansiirtojärjestelmässä raha muunnetaan elektroniseksi kolikoksi, joka on digitaalisten allekirjoituksien jono (Abrazhevich et al. 2001; Nakamoto 2008). Elektronisten kolikoiden takia rahoituslaitoksen ei tarvitse pitää hallussaan vastaavaa määrää käteisvaluuttaa (Panurach 1996). Elektroninen transaktio tapahtuu, kun kolikon omistaja siirtää kolikon seuraavalle omistajalle. Transaktiossa omistaja allekirjoittaa

digitaalisesti edellisen transaktion tiivistelmän ja hyväksyy seuraavan omistajan julkisen avaimen, eli osoitteen minne raha lähetetään. Näin maksun saaja voi tarkistaa kolikon omistuksen jonon ja hyväksyä transaktion digitaalisella allekirjoituksellaan eli salaisella avaimellaan. (Abrazhevich et al. 2001; Nakamoto 2008; O'Mahony et al. 2001; Panurach 1996) Käytännössä luotettu kolmas osapuoli tarkistaa kolikon omistuksen, eikä maksun saaja itse. Lähetettävä kolikko on siis salattu julkisella tai salaisella avaimella (Panurach 1996). Transaktio on havainnollistettu kuvassa 3. Ongelmaksi muodostuu, että maksun saaja ei voi tarkistaa onko kyseinen kolikko jo käytetty (Nakamoto 2008). Tällaisissa tilanteissa ainoastaan yksi maksunsaajista saa kolikon viimekädessä haltuunsa, kuten kuvassa 2 on havainnollistettu.



Kuva 3. *Elektronisen kolikon transaktio, mukailtu lähteestä (Nakamoto 2008 s.2)*

Kyseinen ongelma on ratkaistu tuomalla transaktioon luotettu kolmas osapuoli (Malinova & Park 2016). Kyseinen kolmas osapuoli, kuten pankki, tarkistaa elektronisen kolikon kahdenkertaisen käytön. Kun nykyinen omistaja lähettää kolikon seuraavalle omistajalle, raha kulkee pankin oman järjestelmän kautta. Pankki varmistaa, ettei kolikkoa ole käytetty enempää kuin yhden kerran. Pankki siirtää kolikon niin sanottuun elektroniseen rahapainoon. Rahapainosta lasketaan liikkeelle uusi tuore kolikko, jonka moninkertainen käyttö ei ole mahdollista. Tähän kolikkoon kolmas osapuoli, kuten pankki luottaa. Näin transaktion vastaanottaja saa varmasti siirrettävän rahan (O'Mahony et al. 2001; Nakamoto 2008; Abrazhevich et al. 2001). Ongelma tässä ratkaisussa on se, että koko rahajärjestelmän kohtalo on riippuvainen rahapainoa johtavasta yrityksestä (Nakamoto 2008).

Näitä maksuepävarmuuksia ja niiden luomia kustannuksia ei synny pääoman siirroissa, jotka suoritetaan henkilökohtaisesti fyysisellä rahalla. Lohkoketjuteknologiassa transaktio perustuu kryptografiaan eli salaukseen eikä luottamukseen, mikä on mahdollistettu hajautetulla ja julkisella tilikirjajärjestelmällä (Nakamoto 2008; Franco 2014 s.15; Betancourt 2013; Dai 1998). Kun uusi transaktio tapahtuu, toiminta tarkistetaan niin sanotulla työn varmennusprotokollilla ennen kuin transaktio päivitetään lohkoketjuun (Nakamoto 2008; Franco 2014 s.101). Tämä teknologia on suunnattu juuri digitaalisille valuutoille (Tasca et al. 2016), joka siis ratkaisee Byzantinen kenraalin ongelman verkossa tapahtuvissa transaktioissa (Dourado & Brito 2014; Betancourt 2013). Lohkoketjuteknologia siis mahdollistaa kahdenvälisen kaupan ilman luotettua kolmatta osapuolta (Betancourt 2013). Kaikki Bitcoin lohkoketjua aikaisemmat kahdenväliseen kauppaan tarkoitetut kryptovaluutat ja järjestelmät ovat kaatuneet valuutan moninkertaiseen käyttöön (Dourado & Brito 2014).

3. LOHKOKETJUTEKNOLOGIA

Lohkoketjuteknologia on alun perin suunniteltu juuri kryptovaluutoille, kuten Bitcoinille (Dourado & Brito 2014; Nakamoto 2008; Maineli & Smith 2015). Lohkoketjuteknologia mahdollistaa todelliset kahden osapuolen väliset transaktiot. Tämä on mahdollista hajautetun mallin kautta, jossa transaktiot suojataan kehittyneellä kryptografialla ja tarkistetaan hajautetun tilikirjajärjestelmän kautta. (Malinova & Park 2016)

Internet-pohjainen teknologia mahdollistaa kitkattoman informaation vaihdon, kun taas lohkoketjuteknologia mahdollistaa kitkattoman pääoman vaihdon. Pohjimmiltaan lohkoketju on kaikkien tapahtumien tilikirja, jota pidetään julkisessa, levinneessä sekä yleisesti helppopääsyisessä verkossa. (Malinova & Park 2016; Mainelli & Smith 2015; Böhme et al. 2015) Lohkoketjussa transaktiot verifioidaan yhdistämällä tapahtuman molempien päiden niin sanotut julkiset avaimet, mitä voi ajatella anonyymeina tunnisteina (Diffie & Hellman 1976; Malinova & Park 2016; Mainelli & Smith 2015). Kun julkiset avaimet on yhdistetty, transaktion tarkistus tapahtuu niin kutsuttujen työn varmennusprotokollien kautta, jossa lukuisat louhijat kilpailevat maksun tarkastamisesta (Malinova & Park 2016; Mainelli & Smith 2015). Louhiminen sekä varmennusprotokollat esitellään tarkemmin tässä kappaleessa.

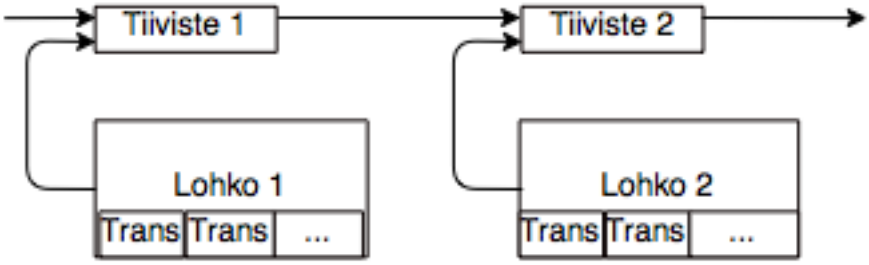
Lohkoketjuteknologia nähdään uutena yleiskäyttöteknologiana (Bresnahan & Trajtenberg 1995; Lipsey et al. 2005), joka on erittäin läpinäkyvä, joustava sekä toimii hajautetun tietokannan kautta (Maineli & Smith 2015; Pilkington 2016). Lohkoketjuteknologia on siis yleiskäyttöteknologia, josta polveutuu monia spesifimpiä innovaatioita moneen eri käyttötarkoitukseen (Pilkington 2016). Suurin osa uusista lohkoketjupohjaisista innovaatioista on suuntautunut keskitettyjen järjestelmien korvaamiseen. Laajalle hajautettuja tietokantoja voidaan soveltaa keskitettyjä järjestelmiä tehokkaammin luotettavaan tiedonsiirtoon. Lohkoketjun rakenteen takia uudet innovaatiot eroavat usein instituutioiden hallinnollisesta muodosta. Jotta uudet innovaatiot toimisivat, instituutioiden hallintarakennetta täytyisi muuttaa. (Wright & De Filippi 2015; He et al. 2016; Tasca et al. 2016) Muutos keskitetystä tietojärjestelmästä hajautettuun, muuttaisi siis koko instituution rakennetta (Tasca et al. 2016).

3.1 Aikaleimaverkko ja työn varmennusprotokolla

Lohkoketjuteknologia hyödyntää aikaleimaverkkoa, joka toimii ottamalla tiivisteen lohkoketjun sisältämästä informaatiosta ja julkaisemalla tiivisteen lohkoketjuyhteisöön (Massias et al 1999; Haber & Stornetta 1991; Bayer et al. 1993 s. 329; Haber & Stornetta 1997). Toisin sanoen lohkon sisältämä informaatio on siis julkista tietoa, kuten esimerkiksi sanomalehtikirjoitukset. Nakamoton (2008) mukaan aikaleima todistaa, että

datan on pitänyt olla olemassa tiettynä ajanhetkenä, jotta se on päätynyt tiivisteeseen. Jokainen aikaleima sisältää aikaisemman aikaleiman tiivisteessään muodostaen aikaleimoista ketjun. Jokainen aikaleima vahvistaa edellisten aikaleimojen sisällön, joka lisätään ketjuun.

Kuva 4 esittää aikaleimoista muodostuvaa ketjua. Kuvassa lohkojen sisältämä informaatio, kuten transaktiotiedot on aikaleimattu ja ne ovat päätyneet tiivisteisiin. Kuvassa 4 tiiviste 2 vahvistaa vasemmanpuolisen tiivisteen 1 tiedot ja sisäistää ne itseensä muodostaen ketjun. Tämä ketju muodostaa kokonaisuudessaan laajan aikaleimaverkon, jossa transaktiotiedot ovat lukemattomia kertoja lukuisissa tiivisteissä.

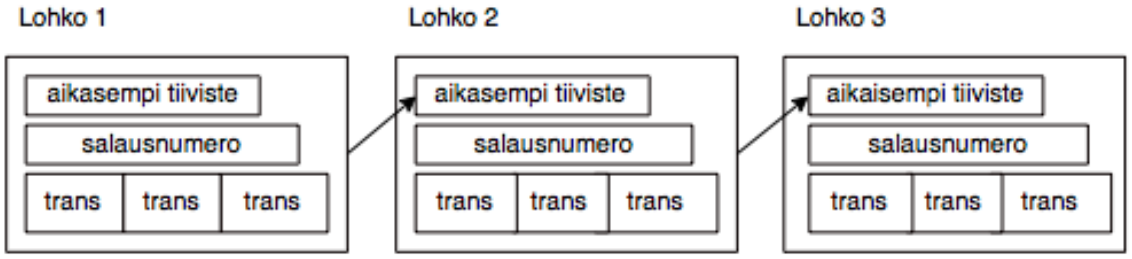


Kuva 4. *Aikaleimaverkko, mukailtu lähteestä (Nakamoto 2008, s. 3)*

Jotta aikaleimaverkko toimii, transaktioiden aitous pitää pystyä todistamaan. Tähän ongelmaan on kehitetty työn varmennusprotokolla. Tämä varmennusprotokolla etsii tiettyä arvoa tiivisteelle, joka alkaa tietyllä määrällä nolla-bittejä. Tiiviste muodostetaan kryptografisella tiivistefunktiolla nimeltään SHA-256, jonka tiivisteen pituus on 256 bittiä. Tiiviste siis tiivistää transaktioinformaation niin, ettei sitä saa enää muutettua alkuperäiseen muotoon. Tiivistetty informaatio pysyy kuitenkin luettavassa muodossa. Tarvittava keskimääräinen laskentatyön määrä kasvaa eksponentiaalisesti tarvittavien nolla-bittien lukumäärään kasvaessa. Nolla-biteillä todennetaan työnalla oleva tiiviste. (Nakamoto 2008)

Aikaleimaverkosto toteutetaan työn varmennusprotokollan avulla kasvattamalla salausnumeroa lohkossa. Salausnumeroa kasvatetaan, kunnes löydetään arvo, joka antaa lohkon tiivisteelle tarvittavat nolla-bitit. Kun salausnumeron laskettu arvo antaa oikeat nolla-bitit työn varmennusprotokollan mukaisesti, lohkoa ei voida muuttaa muulla tavalla kuin aloittamalla salausnumeron laskeminen uudestaan. Tiivistämisen jälkeen lohkot ketjutetaan toisiinsa, jolloin yhden lohkon muuttaminen vaatisi jokaisen kyseistä lohkoa seuraavan lohkon muuttamista. (Nakamoto 2008)

Kuva 5 kuvastaa, miten transaktioinformaatio tallentuu uuden lohkon tiivisteeseen. Näin lohkot ovat yhteydessä toisiinsa ja sisältävät kaikki aikaisemmat lohkojen tallentamat informaatiot tiivisteissään. Toisin sanoen lohkon 1 transaktiotiedot voidaan tarkistaa lohkosta 3.



Kuva 5. *. Datan arkistointi lohkoketjuteknologiassa, mukailtu lähteestä (Nakamoto 2008, s.3)*

Varmennusprotokolla ratkaisee myös enemmistöpäätökseen liittyvät ongelmat. Oikean salausnumeron äänestys perustuu siihen, että jokaisella tietokoneen keskusmuistilla on yksi ääni käytettävissä. (Nakamoto 2008; Böhme et al. 2015) Jos enemmistö perustuisi IP-osoitteeseen, kuka tahansa voisi horjuttaa äänestystä allokoimalla monia IP-osoitteita samaan aikaan. Enemmistöpäätöksen laskennallisesta arvosta esittää ketju, jolla on pisin luotettava varmennusprotokolla historia. Jos rehelliset klusterit, jotka ovat usean tietokoneen verkotettuja malleja, hallitsevat suurinta osaa laskenta tehosta, rehellinen ketju kasvaa nopeimmin, ja voittaa kaikki kilpailevat ketjut. Muokatakseen mennyttä lohkoa, hyökkääjän täytyisi suorittaa uudestaan varmennusprotokolla muokattavassa lohkossa sekä kaikissa muissa sen jälkeisissä lohkoissa. Sen lisäksi hyökkääjän tulisi yltää tehdyssä työssä rehellisten tasolle ja nousta vielä tämän tason yli. Todennäköisyys hyökkääjän onnistumisesta edellä mainituissa seikoissa pienenee eksponentiaalisesti, kun seuraavia lohkoja lisätään ketjuun. (Nakamoto 2008)

Lohkoketjun laskentatehon lisääntyessä varmennusprotokollan vaikeusaste kasvaa (Nakamoto 2008). Toisin sanoen salausnumeron kryptografinen lasku vaikeutuu lineaarisesti laskentatehon kasvaessa. Nakamoton (2008) mukaan klustereiden laskentatehon ja intressien vaihdellessa varmennusprotokollan vaikeuteen vaikuttaa myös liukuva keskiarvo. Kyseinen liukuva keskiarvo pyrkii saavuttamaan keskimääräisen nopeuden (lohkoa per tunti) muihin lohkoihin verrattuna. Jos lohkoja luodaan liian nopeasti varmennusprotokollan vaikeusaste kasvaa, jolloin lohkojen luominen hidastuu. (Nakamoto 2008) Toisin sanoen laskentatehon kasvaessa varmennusprotokolla vaikeutuu ja taas laskentatehon laskiessa vaikeustaso laskee. Optimaalinen lohkojen valmistumistahti esimerkiksi Bitcoinille on yksi lohko kymmenessä minuutissa (Nakamoto 2008).

3.2 Louhinta

Kryptovaluuttojen louhinta on prosessi, jossa transaktiot verifioidaan ja lisätään julkiseen tilikirjaan eli lohkoketjuun (Fanning & Centers 2016; Pinna & Ruttenberg 2016). Louhinnassa kilpaillaan transaktion verifioinnista, jossa lasketaan varmennusprotokollan antamaa salausnumeroa (Nakamoto 2008). Salausnumero on salattu hankalalla kryptografisella ongelmalla, jolla turvataan lohkon turvallisuus. Louhinta on toisin

sanoen kilpailullista tilikirjan luontia, missä lohko lisätään vasta silloin kun oikea tulos on löytynyt. (Harvey 2014) Uusi lohko lisätään noin kymmenen minuutin välein lohkoketjuun (Nakamoto 2008; Harvey 2014; Pinna & Ruttenberg 2016), joten kilpailu oikeasta vastauksesta alkaa joka kymmenes minuutti. Louhimisaspekti mullistutti koko lohkoketjuteknologian ratkaisemalla edellä mainitun Byzantinin kenraalin ongelman transaktioiden verifioinnissa (Maineli & Smith 2015).

Louhinta koostuu hajanaisista klustereista, jotka koostuvat yksittäisistä louhijoista (Fanning & Centers 2016). Louhijat käyttävät tietokoneiden tai serverien laskentatehoa transaktioiden verifioimiseen, jonka yhteydessä syntyy lisää kryptovaluuttaa, kuten Bitcoinia. Uudella kryptovaluutalla palkitaan louhija, joka saa ensimmäisenä laskettua oikean tuloksen. Ennen palkitsemista tulos varmennetaan vertaamalla sitä muiden tuloksiin. Jos suurin osa louhijoista on samaa mieltä tarkasteltavan tuloksen kanssa, tulos hyväksytään, louhija saa palkinnon työstään ja lohko lisätään lohkoketjuun. (Harvey 2014; Pinna & Ruttenberg 2016) Palkintokryptovaluutat ovat seuraavan lohkon ensimmäinen transaktio (Fanning & Centers 2016).

Louhiminen tapahtuu usein niin sanotuissa louhimisringeissä, joissa louhijat yhdistävät laskentatehonsa. Jos louhimisrinki onnistuu ratkaisemaan ensimmäisenä kryptografisen ongelman, palkinto jaetaan ringin kesken laskentatehon mukaan. (Harvey 2014) Louhinta suoritetaan usein tietokoneen keskusprosessorilla tai näytönohjaimella Internetin välityksellä (Fanning & Centers 2016). Louhinnassa käytetään paljon laskentatehoa (Pinna & Ruttenberg 2016). Harveyn (2014) mukaan Bitcoinia louhittiin 9 800 000 petaFLOPsin laskentateholla. Sen ajan tehokkain supertietokone NUDT Tiahne-2, jonka laskentateho on 33,9 petaFLOPSia. Verrattaessa laskentatehoja keskenään, tarvittaisiin 300 000 kappaletta vuoden 2014 tehokkainta supertietokonetta vastaamaan laskentatehoon, mitä Bitcoinin louhinnassa käytetään. Bitcoinin lohkoketjun murtamiseen tarvitsisi siis valtavasti laskentatehoa, jonka hankkimisessa onnistuminen vaikuttaa hyvin epätodennäköiseltä (Pinna & Ruttenberg 2016).

Louhijat siis turvaavat avoimien transaktiotietojen turvallisuuden lohkoketjussa (Harvey 2014; Pinna & Ruttenberg 2016). Samalla transaktioista muodostuvat lohkot tallentuvat louhijoiden tietokoneille. Jokainen klusteri säilyttää koko lohkoketjun transaktiohistorian ja samalla tarkistaa uusia transaktioita. Työn varmennusprotokolla siis varmistaa uusien transaktioiden virheettömyyden sekä varmistaa, että konsensus on olemassa kaikkien klustereiden välillä. Lohkoketjun yhdenmukaisuus ja yhdenmukaisuuden säilyminen ovat koko varmennusprotokollan ydin. Tällä turvataan, että uudet lohkot ovat yhteydessä edellisiin lohkoihin, ja kaikki lohkot ovat yhdenmukaisia yhdessä jatkuvassa ketjussa. (Yli-huumo et al. 2016; Nakamoto 2008) Lohkoketju siis kasvaa lineaarisessa sekä

kronologisessa järjestyksessä muodostaen lohkoista muodostuvan ketjun (Fanning & Centers 2016).

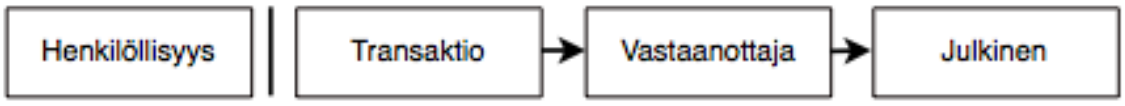
Ylikasvaneet louhimisringit vaarantavat kuitenkin hajautetun järjestelmän luottamusta. GHash niminen louhimisrinki ylitti 50 prosentin laskentatehon osuuden Bitcoinin louhimisessa kesällä 2014. Ylitys kesti vain kaksitoista tuntia, mutta GHash olisi voinut manipuloida lohkoketjua tänä aikana. (Böhme et al. 2015)

3.3 E-tili ja yksityisyysmalli

Kryptovaluuttoja säilytetään niin sanotuissa elektronisissa lompakoissa, jotka ovat datatiedostoja. Lompakko sisältää kryptovaluuttatilin, transaktiotiedot, julkisen sekä salatun avaimen. Tietokoneen kaatuminen tai hyökkäys kyseiselle tietokoneelle, jossa elektroninen lompakko on tallennettu, voi johtaa kryptovaluutan tuhoutumiseen. Tästä syystä monet kryptovaluutan käyttäjät pitävät elektronista lompakkoa jaetulla serverillä, johon pääsee käsiin internetin välityksellä. Elektronisen lompakon tarjoajat hoitavat edellä mainittujen tiedostojen säilyttämisen, mutta eivät omista salaista avainta. Näin palvelun tarjoaja ei voi hallita asiakkaan omistamia kryptovaluuttoja. (Böhme et al. 2015)

Monet elektroniset maksujärjestelmät tarjoavat menetelmiä suojelemaan asiakkaitaan luvattomilta transaktioilta ja suoja on useassa tapauksessa lain määräämä. Kryptovaluuttojen uutuudesta johtuen asiakkaan suojaa ei vaadita laissa, jolloin palvelun tarjoajilla ei ole tarjota suojaa asiakkaalle. Suojan puuttuminen kryptovaluutoissa näyttää olevan vastoin vanhaa yhteiskuntapolitiikkaa. (Böhme et al. 2015)

Lohkoketjun käyttämä yksityisyysmalli turvaa käyttäjän henkilöllisyyden, mutta transaktiot ja niiden osapuolet (julkiset avaimet) ovat julkista tietoa. Kuvassa 6 on mallinnettu uusi yksityisyysmalli, jossa pystyviiva kuvaa palomuuria. Palomuuri erottaa yksityisen tiedon, kuten asiakkaan henkilöllisyyden, ja julkisen tiedon, kuten transaktiotiedot.



Kuva 6. *Uusi yksityisyysmalli, mukailtu lähteestä (Nakamoto 2008 s.6)*

Hajautetut mallit ovat kalliita ja niissä on usein merkittäviä luottamusongelmia. Vasta viime vuosina hajautetun mallin luottamusongelma on saatu ratkaistua tehokkaasti. Lohkoketju ratkaisi ongelman korvaamalla luottamuksen kehittyneellä salauksella ja konsensusmekanismilla. Kryptografiaan perustuva järjestelmä ei tarvitse luotettua kolmatta osapuolta vahvistamaan transaktiota, jolloin kolmannen osapuolen merkitys

katoaa lohkoketjujärjestelmässä. Lohkoketjun turvallisuus on pysynyt vakaana jopa vahvojen tai vihamielisten kolmansien osapuolien seurassa. (Tasca et al. 2016)

3.4 Transaktio ja kustannukset

Transaktiokustannukset lohkoketjupohjaisissa kryptovaluutoissa ovat hyvin alhaiset. Tämä johtuu siitä, että pääoman siirtoon ei tarvitse erillisiä lupia (Thierer 2014; Tasca et al. 2016). Lohkoketjussa pääomaa ei siirretä toisesta instituutioista toiseen eikä esimerkiksi USA:n osavaltioiden asettamat kauppaesteet tai verotukset vaikuta lohkoketjuun. Varsinkaan valtioiden tai liittoumien väliset kauppasopimukset tai verot eivät vaikuta lohkoketjun toimintaan, koska lohkoketjupohjaiset kryptovaluutat toimivat alueettomasti. Tämä johtuu siitä, että lohkoketjut toimivat Internetin välityksellä, eikä Internet ole keskitetty mihinkään tiettyyn alueeseen. (Tasca et al. 2016) Transaktiokustannus muodostuu tai tulee muodostumaan ainoastaan työnvarmennusprotokollan ratkaisun saaneesta louhijasta. Esimerkiksi Bitcoinin tilanteessa transaktiokustannuksia ei muodostu maksujärjestelmän osapuolille vielä, koska louhija saa korvauksen kolikoista/kolikosta, mitä ei ole vielä julkaistu markkinoille. Bitcoineja tulee olemaan rajallinen määrä (21 miljoonaa), mutta kyseinen raja ei ole tullut vielä vastaan. (Nakamoto 2008)

Lohkoketjupohjaisissa transaktioissa on myös huonoja puolia. Esimerkiksi Bitcoinin lohkoketjuun muodostuu uusi lohko noin 10 minuutin välein. Tämä mahdollistaa potentiaalisen riskin, ettei lohkoa hyväksytäkään lohkoketjuun enemmistöäänestyksessä, jolloin kaikki lohkon sisältämät transaktiot peruutetaan. (Böhme et al. 2015)

Pääoman vapaaseen kulkuun lohkoketjussa liittyy myös huonoja puolia. Mikään valtio tai taho ei voi vaikuttaa kryptovaluuttojen liikenteeseen, mikä mahdollistaa rikollisen toiminnan. (Tasca et al. 2016) Lohkoketjupohjaisissa järjestelmissä ei siis ole hallinnollista järjestelmää. Tästä seuraa, ettei transaktioita voida hallita millään tavalla, joka mahdollistaa esimerkiksi laittomien tuotteiden tai palvelujen ostamisen. Transaktiot ovat myös peruuttamattomia, koska protokolla ei tarjoa mitään keinoa maksajalle peruuttaa tahatonta tai ei toivottua ostosta. (Böhme et al. 2015) Lohkoketjupohjaisista maksupalveluista puuttuu siis kokonaan keskeinen sovittelija (Nakamoto 2008: Harvey 2015), joka voisi korjata transaktioissa tapahtuneet virheet.

Lohkoketjupohjaiset transaktiot lakkaisivat toimimasta, jos julkisen avaimen salaus murrettaisiin. Myös Internetin kaatuessa kokonaan, kryptovaluutat lakkaisivat toimimasta kuten kaikki muu nykyaikaisessa rahoituksessa käytettävät maksupalvelut kuten luottokortit. (Maineli & Smith 2015)

4. TULOSOSIO

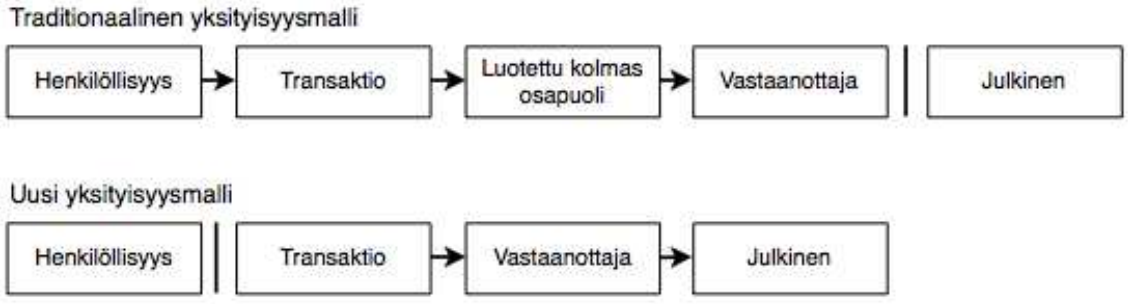
Tässä luvussa vertaillaan nykyistä pankkijärjestelmää ja lohkoketjuteknologiaa keskenään. Vertailun kohteena on järjestelmien eri aspektit, kuten informaation tallentamismenetelmät. Tulososiossa siis keskitytään järjestelmien transaktiomenetelmien vertailemiseen ja niiden eroihin. Maksujärjestelmien eri osia tarkastellaan rinnakkain ja analysoidaan osakokonaisuuksien vahvuuksia ja heikkouksia.

Vertailusta seuranneita eroavaisuuksia analysoidaan luvun loppupuolella lohkoketjun nykyisen käyttöasteen kautta. Luvussa myös pohditaan, miten lohkoketjuteknologia voisi muuttaa rahoitusalaa sekä mikä osa-alue voisi hyötyä lohkoketjuteknologiasta.

4.1 Keskitetty malli verrattuna hajautettuun malliin

Ensimmäisenä vertailukohteena ovat järjestelmien yksityisyysmallit sekä informaation tallentamismenetelmät. Edellä mainittuihin aspekteihin liittyy merkittävästi keskitetyn ja hajautetun järjestelmän tarkasteleminen.

Kuvassa 7 on asetettu traditionaalinen yksityisyysmalli uuden yksityisyysmallin kanssa rinnakkain. Mallien eroavaisuus on merkittävää järjestelmien erilaisen toiminnan vuoksi. Traditionaalisessa järjestelmässä luotetulla kolmannella osapuolella on kaikki transaktioon liittyvä informaatio, mutta se rajaa tiedon julkisuudesta. Uudessa yksityisyysmallissa ainoastaan käyttäjien henkilöllisyys on rajattu pois julkisesta tiedosta. Näin transaktiotiedot ovat kaikkien ulottuvilla, mutta anonyyminä. Jos julkiset avaimet saadaan yhdistettyä henkilöllisyyteen lohkoketjun anonyymisyys sekä avoimen tilikirjan idea katoaa kokonaan (Nakamoto 2008).



Kuva 7. *Yksityisyysmallien vertailu, mukailtu lähteestä (Nakamoto 2008 s.6)*

Monimutkaisilla järjestelmillä on taipumus kehittyä keskitetystä mallista hajautettuun malliin. Monet järjestelmät aloitetaan keskitetyllä mallilla, koska tämä malli on tehokkain tietorakenteiden luomiseen, julkaisemiseen sekä valvomiseen. Keskitetty järjestelmä minimoi kopioimista, esittää selkeän hierarkian järjestelmän sisällä sekä voi ratkaista

tehokkaasti kiistoja. Nämä samaiset keskitetyn mallin vahvuudet altistavat järjestelmän väärinkäytön. Esimerkiksi talousjärjestelmissä keskitetyn mallin vahvuudet mahdollistavat inflaation, korruption ja välistävedon kuten toisessa luvussa esiteltiin. Keskitetyn järjestelmän kasvaessa väärinkäytön riskit sekä järjestelmän ylläpitokustannukset kasvavat. Keskitetyn mallin kustannuksiin ja väärinkäytön riskiin verrattuna hajautetun mallin riski sekä kustannukset laskevat järjestelmän kasvaessa. Tämä johtuu usein teknologisesta kehityksestä. (Tasca et al. 2016).

Nykypäivän rahoitusmarkkinoiden yhteisen ”kultaisen tilikirjan” päivittäminen monien keskitettyjen järjestelmien välillä on siis työlästä. Samasta yhteisestä tilikirjasta on lukuisia kopioita ympäri tietojärjestelmää. Lisäksi rahoituksen välittäjien täytyy päivittää omat tilikirjansa aina, kun uusi transaktio tapahtuu. Luotettuja kolmansia osapuolia vaaditaan lähettämään kaikkia olennaisia tietoja transaktiosta asianomistajille ja jälkikaupan teollisuuden eri tahoille. Lähetettyä tietoa sovitetaan yhteen muiden kolmansien osapuolien omien transaktioiden kanssa, jotta voidaan heijastaa uutta tilannetta ja informoida niiden asianomistajia kaikista muutoksista. (Pinna & Ruttenberg 2016) Yhteisen tilikirjan ylläpitäminen on siis haastavaa nykyisessä järjestelmässä verrattuna lohkoketjuteknologian tarjoamaan tapaan.

Luotettavan kolmannen osapuolen tehtäviin kuuluu pääoman validointi, turvaaminen ja säilyttäminen. Jos käyttäjien luottamus hajautettuun tilikirjajärjestelmän koskemattomuuteen saavutetaan, lohkoketju voisi suurelta osin syrjäyttää luotetun kolmannen osapuolen kaksi tehtävää, turvaaminen ja säilyttäminen. Lohkoketjulla näin turvattaisiin, ettei rahan moninkertaista käyttöä tapahdu, sekä varmistettaisiin todenmukaisen julkisen tilikirjan saanti kaikista tapahtumista. Edellä mainitut voivat myös lisätä validoinnin tärkeyttä. Validointi siis valvoo nykymarkkinoita ja yhteisön jäsenien luotettavuutta. Lisääntynyt luottamus hajautettuun järjestelmään mahdollisesti alentaa luotettavien kolmansien osapuolien alalle pääsyn esteitä, kustannuksia ja samalla lisää kysyntää. (Maineli & Smith 2015)

Kuten modernissa rahataloudessa, jossa rahaa pidetään sähköisessä muodossa, pääoman niukkuus luo kysynnän ja tarjonnan suhteen. (Böhme et al. 2015) Keskuspankilla on valta säätää absoluutista rahamäärää markkinoilla (Böhme et al. 2015), mikä luo merkittävän voimakeskittymän. Hajauttaminen tarjoaa tiettyjä etuja. Se välttää voimakeskittymiä, jotka voivat antaa yhden henkilön tai organisaation ottaa omaan päätäntövaltaansa esimerkiksi koko tilikirjahistorian (Böhme et al. 2015). Hajauttaminen myös edistää tietojärjestelmän saatavuutta ja joustavuutta varsinkin kehitysmaissa (Böhme et al. 2015; Yermack 2017). Lohkoketjuteknologialla on potentiaalinen mahdollisuus parantaa miljoonien ihmisten elämää, joilla ei ole pankkitilejä tai pääsyä oikeudelliseen ja hallinnolliseen infrastruktuuriin (Dandapani 2017).

Hajautettu järjestelmä ei vaadi leviämiseen samanlaisia resursseja kuin keskitetty ja järjestelmän kaatuminen vaatisi koko Internetin kaatumista (Böhme et al. 2015).

Keskitetyistä järjestelmistä poiketen verkon toiminnot säilyvät, vaikka tietyt solmut hajoaisivat. Tämä lisää luottamusta, koska käyttäjien ei tarvitse arvioida välittäjän tai muiden verkon osanottajien luotettavuutta. Riittää, jos ihmiset rakentavat luottamuksensa järjestelmään kokonaisuutena. Luotetun kolmannen osapuolen puuttuminen edistää myös tietoturvaa. (Nofer et al. 2017) Samalla lohkoketjuteknologia tarjoaa aidon ja paremman yksityisyyden, kuin keskitetty järjestelmä (Böhme et al. 2015; Nakamoto 2008). Hajautetussa järjestelmässä käyttäjien tietoja on hyvin vaikea kerätä verrattuna keskitettyyn järjestelmään (Nofer et al. 2017).

Hajautetun ja keskitetyn tietojärjestelmän tietoturvallisuus riippuu tietoturvahyökkäyksen muodosta. Keskitettyyn tietojärjestelmään hyökätessä pyritään saamaan koko serveri haltuun. Tällöin koko järjestelmä on hyökkääjien hallinnassa. Taas hajautettuun tietojärjestelmään hyökätessä, hyökkäykset pitää kohdistaa yhteen kolmasosaan louhinnan varmennusprotokollan tuloksen tarkastajista. Kun kolmasosa on hyökkääjien hallinnassa, he pystyvät manipuloimaan hajautettua tietojärjestelmää. Keskitetyissä järjestelmissä on usein tietoturvallisuusstandardeja, joita hajautetun järjestelmän varmennusprotokollan tarkastajilta ei vaadita. (Pinna & Ruttenberg 2016)

Toisaalta esimerkiksi hajautetun järjestelmän päätäntäprosessi, jossa monien osapuolten on päästävä yhteisymmärrykseen, rajoittaa ratkaisun nopeutta verrattuna keskitetysti hallinnoidun tietojärjestelmän avulla saavutettuun nopeuteen. (Pinna & Ruttenberg 2016)

Siirtyminen yhdestä institutionaalisesta systeemistä toiseen, esimerkiksi rahoitusmarkkinoilla pankkiorganisaatiosta lohkoketjupohjaiseen rahoitusjärjestelmään ei tapahdu ilman kustannuksia (Pagano & Vatiero 2015). Muutos nähdään tapahtuvan metainstituutionaalisten muutoskulujen kautta. Kustannukset vastaavat tietojärjestelmän rakenteen uusimisesta sekä muutoskustannuksista. Samalla pääoman on vaihdettava muotoa elektronisista kolikoista pankin valitsemaan kryptovaluuttaan. (Tasca et al. 2016) Pankkien kryptovaluutaksi sopisi esimerkiksi kansainväliseen pankkiliiketoimintaan kehitetty kryptovaluutta Ripple (Pinna & Ruttenberg 2016).

4.2 Transaktiot

Lohkoketju kehittyy jatkuvasti, jolloin teknologian kustannuskäyrä laskee voimakkaasti. Toisin sanoen lohkoketjuteknologian kehittyessä siitä tulee potentiaalinen haastaja ja jopa korvaaja kypsälle keskitetylle mallille. Transaktiokustannuksissa säästäminen on yksi suurimmista kilpailun kohteista järjestelmien välillä. (Tasca et al. 2016)

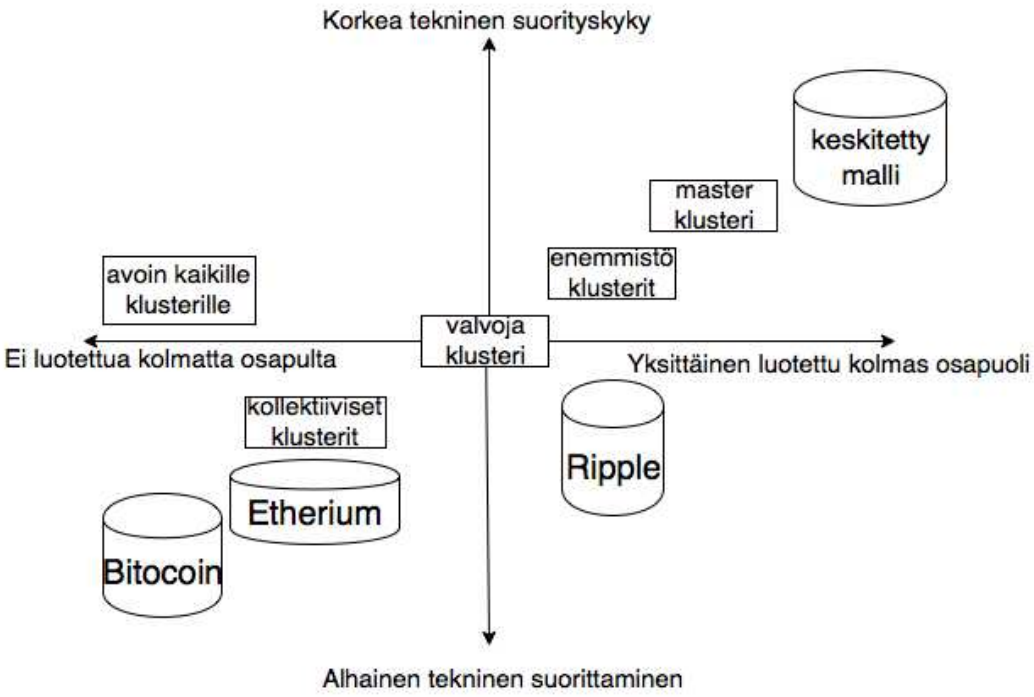
Pankit ovat pystyneet toimimaan taloudellisesti suhteellisen tehokkaasti. Kuitenkin lohkoketjuteknologian tarjoamat, kryptografiasuojatut ja hajautetut tilikirjat alentavat entisestään perustransaktiokustannuksia rahoitusomaisuudelle. Tämä vaikuttaa merkittävästi pankkien toimintaan, sillä pankkitoiminta perustuu suurelta osin markkinoita palvelevaan tehokkaaseen rahanvaihtoon. (Tasca et al. 2016)

Lohkoketjuteknologia mahdollistaa niin alhaiset transaktiokustannukset, etteivät perinteiset pankit pysty kilpailemaan enää kustannuksien kanssa.

Kuluttajan näkökulmasta vaikuttaisi luonnolliselta käyttää esimerkiksi Bitcoinia kansainvälisiin transaktioihin, koska perinteistä järjestelmää käyttäessä transaktiokustannukset voivat nousta yli 50 dollariin (Nakamoto 2008; Böhme et al. 2015; Harvey 2014) ja maksun hyväskymispäätöksessä voi kestää useita päiviä (Nofer et al. 2017). Toisaalta esimerkiksi Bitcoin tuskin tulee vielä korvaamaan pankki- tai luottokorttia, johon sisältyy muun muassa kuluttajan suoja ja transaktioiden riitauttaminen (Pinna & Ruttenberg 2016; Nakamoto 2008; Böhme et al. 2015; Harvey 2014). Lohkoketjuteknologia ei pysty kilpailemaan riitauttamisen tai hyvityksen suhteen ollenkaan peruuttamattomien transaktioidensa takia (Pinna & Ruttenberg 2016; Harvey 2014). Nykypäivän kryptovaluuttojen transaktioliikennettä ei siis pysty kontrolloimaan tai rajoittamaan, mikä on muun muassa mahdollistanut maailmanlaajuisen satojen miljoonien dollarien huumekaupan Tor-verkon välityksellä. Anonyymiyden sekä vaikeasti jäljitettävyyden takia kryptovaluutat mahdollistavat tehokkaan rahanpesun. Myös Bitcoin pohjaisia uhkapelisivustoja löytyy sadoittain Internetistä. (Böhme et al. 2016) Kryptovaluuttojen toimintaperusteet anonyymisyys ja hallitsemattomuus mahdollistavat siis rikollisen toiminnan, jota on hankala estää.

Suosituin kryptovaluutta Bitcoin pystyy tekemään noin seitsemän transaktiota sekunnissa, kun taas esimerkiksi Visa pystyy suorittamaan noin 2 000 transaktiota sekunnissa (Yli-Huumo et al. 2016). Kuitenkin muut kryptovaluutat, kuten Etherium ja Ripple ovat luotu skaalautumaan maailmanlaajuiseen kaupankäyntiin (Pinna & Ruttenberg 2016; Fanning & Centers 2016).

Kuva 8 demonstroi, kuinka eri järjestelmät hyödyntävät teknistä suorituskykyä ja kuinka avoimia järjestelmät ovat. Kuvan oikeassa yläkulmassa on nykypäivän rahoitusalan käyttämä keskitetty malli. Keskitetty malli hyödyntää niin sanottua Master klusteria, eli pankin omaa serveriä, joka ylläpitää järjestelmää. Kuvasta nähdään, että keskitetyllä järjestelmällä on hyvin korkea tekninen suorituskyky verrattuna muihin järjestelmiin. Tämä tarkoittaa siis sitä, että järjestelmän laskentateho käytetään tehokkaasti järjestelmän toimintojen ylläpitämiseen (Mainelli & Smith 2015). Bitcoinin louhinnassa on taas käytössä todella suuri laskentateho (Harvey 2014), mitä ei saada käytettyä tehokkaasti transaktioiden suorittamiseen (Yli-Huumo et al. 2016). Yli-Huumo et al. (2016) mukaan myös Bitcoinin louhimiseen kuluu noin 15 miljoonaa dollaria päivässä. Bitcoinin louhiminen ei siis ainakaan tällä hetkellä ole energiatehokasta verrattuna nykyiseen pankkijärjestelmään.



Kuva 8. *Arkkitehtuurimallien erot, mukailtu lähteestä (Mainelli & Smith 2015 s.38)*

P2P-markkinoille noussut rahoitusyritysten aalto pyrkii valtaamaan juuri pankkien omistamat välittäjämarkkinat (Tasca et al. 2016). Nämä rahoitusyritykset käyttävät lohkoketjuteknologiaa hyväkseen (Tasca et al. 2016), jolloin he mahdollistavat suoran yhteyden säästäjien ja lainaajien välille ilman pääoman kierrätystä kolmannen luotetun osapuolen kautta. Lohkoketjun uskottavuus ja toimivuus on tunnistettu, jonka seurauksena lohkoketjuteknologiaa on aloitettu implementoimaan monille applikaatioille (Mainelli & Smith 2015).

4.3 Nykypäivän käyttöaste

Rogersin (2003, s.6) mukaan teknolokinen innovaatio hyödyntää informaatiota ja vähentää siten epävarmuutta ongelmanratkaisussa. Lohkoketju soveltuu edellä mainitun teknologisen innovaation määrittelyyn. Lohkoketju esimerkiksi yksinkertaistaa kirjanpitoa ja luo samalla nopean alustan turvallisille transaktioille. Schumpeterin (1942, ss.104-109) disruptiivisen ”Creative destruction” prosessin mukaan, lohkoketju uutena teknologiana on aikaisessa disruptiivisessa vaiheessa. Samalla Clayton et al. (2015) mukaan disruptiivisen innovaation määrittelykriteereihin kuuluu, että innovaation täytyy aloittaa markkinoiden vähiten kannattavimmilla asiakkailla tai luoda täysin uusi asiakaskunta. Lohkoketjuteknologia on onnistunut tekemään molemmat määrittelyn kriteereistä. Toisaalta lohkoketjuteknologia ei ole vielä saavuttanut markkinoiden valtaosaa. Innovaation diffuusion käyrä kehittyy lukuisiksi sovelluksiksi yrittäjien johtamilla markkinoilla teollisen dynamiikan markkinaprosessin mukaan (Schumpeterin 1942, ss.104-109).

Rahoitusmarkkinoilla sekä pankkisetkorilla teknologiapohjainen lähestymistapa on tullut oletusarvoksi, mikä on tehnyt lohkoketjuteknologiasta kiinnostavan investoinnin. (Fanning & Centers 2016; Meijer 2016; Tasca et al. 2016). Pankit hyväksyvät valikoivasti lohkoketjuteknologian johtaen markkinat differentioituneeseen teknologiseen kilpailuun. (Tasca et al. 2016) Tämä muutos voi johtaa vaihtelevampaan ja dynaamisempaan instituution hallintatapaan (Tasca et al. 2016; Yermack 2017).

Chanjaroen & Boey (2016) mukaan petokset neljän biljoonan dollarin rahoitusmarkkinoilla tekevät lohkoketjuteknologiasta hyvin suositun investointikohteen pankeille. Turvatakseen pankkitoiminnan petoksilta uusia liittoutumia syntyy koko ajan pankkien ja uusien lohkoketjuteknologia yhtiöiden välille. Kasvava luottamus on muodostanut merkittävän kiinnostuksen lohkoketjuteknologiaan eri teollisuusaloilla ja varsinkin rahoitusalalla (Tasca et al. 2016; Maineli & Smith 2015). Muun muassa Nasdaq, BNY, Mellon, UBS, USAA, IBM, Samsung ja monet muut ovat investoineet lohkoketjuteknologiaan (Fanning & Centers 2016; Mainelli & Smith 2015). Lohkoketjuteknologian luomat mahdollisuudet ja edut on tunnistettu finanssialalla, ja lohkoketjuteknologian tutkimus on käynnistynyt (Fanning & Centers 2016). Riskisijoittajat ovat innokkaasti investoineet yli 500 miljardia yli sataan startup-yritykseen vuonna 2016, ja arviot vuodelle 2017 ovat vielä korkeammalla. (Fanning & Centers 2016).

Tammikuussa 2016 Australiassa Sydneyn arvopaperipörssi ilmoitti aikomuksestaan uudelleen suunnitella sen arvopapereiden selvitysjärjestelmän. Järjestelmä pohjautuu lohkoketjuteknologiaan. Tätä ennen yhdysvaltalainen arvopaperipörssi NASDAQ sekä saksalainen Frankfurt Deutsche Borsen aloittivat tutkimukset lohkoketjuteknologian hyödyntämisestä arvopaperimarkkinoilla. Lohkoketjun nähdään tuovan potentiaalisia etuja selvitysten ja toimeksiantojen kustannuksissa sekä nopeuksissa. Lohkoketjuteknologiaa käytetään myös äänestysalustana. Virolainen pörssi, joka on NASDAQ:n yksikkö, on alkanut käyttää lohkoketjua osakkeenomistajien äänestysalustana. (Yermack 2017)

Kehittyvien markkinoiden maat saattavat olla ensimmäisiä, jotka implementoivat lohkoketjuteknologian suuressa mittakaavassa omiin pörsseihinsä sekä pääomamarkkinoille. Kehittyvillä valtiolla on monta syytä lohkoketjun varhaiseen adoptioon. Valtioiden nykyiset järjestelmät ovat riittämättömiä, epäluotettavia, korruptoineita sekä tehottomia markkinoiden regulaatioon. (Yermack 2017) Kehitysmaissa älypuhelinten äkillinen suosio on siirtänyt kauppaa internetiin. Esimerkiksi Keniassa mobiilimaksamisjärjestelmät M-Pesa ja BitPesa, jotka toimivat lohkoketjuteknologialla, ovat muodostuneet keskeisiksi maksujärjestelmiksi (Böhme et al. 2015; Yermack 2017). Hondurasin hallitus sekä Georgian tasavalta ovat ilmaisseet halukkuutensa ohittaa länsimaisten käytössä olevan järjestelmän ja implementoida lohkoketjujärjestelmä pitämään kirjaa heidän taloudestaan sekä arvotavaroiden omistuksestaan. (Yermack 2017)

5. YHTEENVETO

Kandidaatintyön pääteemana oli esitellä nykyisen järjestelmän ja lohkoketjuteknologian tarjoamat elektroniset transaktiomenetelmät sekä kyseisten järjestelmien rakenteet, sekä vertailla nykyisen järjestelmän ja lohkoketjuteknologian ominaisuuksia. Työn lopussa tehtiin katsaus nykypäivän käyttöasteesta ja tarkasteltiin rahoitusalan kiinnostusta lohkoketjuteknologiaa kohtaan.

Käytetyn lähdemateriaalin perusteella lohkoketjuteknologia suoriutuu osassa vertailukriteereistä paremmin kuin nykypäivän järjestelmä. Kuitenkin lohkoketjuteknologiasta löytyy heikkouksia, jossa nykyinen järjestelmä suoriutuu paremmin. Vertailukriteerit sekä järjestelmien menestys ovat muodostuneet kirjallisuuskatsauksen perusteella. Järjestelmien menestyminen kussakin vertailukriteereissä on listattu taulukkoon 1. Taulukon vasemmassa sarakkeessa ovat vertailukriteerit, keskisarakkeessa lohkoketjuteknologian menestys vertailukriteereissä ja oikeanpuoleisessa sarakkeessa nykyisen järjestelmän menestys vertailukriteereissä.

Taulukosta 1 nähdään, että lohkoketjuteknologia suoriutuu nykyistä järjestelmää paremmin transaktioiden verifiointinopeudessa ja kustannustehokkuudessa, kirjanpidossa sekä yksityisyydensuojassa. Toisaalta lohkoketjuteknologia mahdollistaa rikollista toimintaa sääntelemättömyytensä sekä anonyymin maksujärjestelmänsä vuoksi. Nykypäivän järjestelmä taas suoriutuu paremmin skaalautuvuudessa, asiakkaan suojaamisessa, transaktioiden riitauttamisessa ja sovittelussa sekä energiatehokkuudessa. Kuitenkin nykyinen järjestelmä mahdollistaa rahan moninkertaisen käytön sekä mahdolliset voimakeskittymät.

Teknologiakeskeinen kilpaileminen rahoitusmarkkinoilla vaatii uusia ratkaisuja. Järjestelmien vertailukriteereiden perusteella rahoitusalan toimijoiden suuret investoinnit lohkoketjuteknologiaan vaikuttavat perusteluilta hankkeilta saavuttaa kilpailuetua markkinoilla.

Kuten taulukosta 1 huomataan, lohkoketjuteknologia ei suoriudu kaikissa vertailukriteereissä pankkijärjestelmää paremmin. Täten lohkoketjuteknologia investoinneilla pyritään korvaamaan vain osa pankkijärjestelmän toiminnoista. Teknologioiden rakenne- sekä toimintaerot ovat kuitenkin merkittäviä, jolloin järjestelmien yhteensovittaminen vaatii suuria muutoksia hallinnossa ja tietojärjestelmissä.

Taulukko 1. *Lohkoketjuteknologia vs. nykyinen järjestelmä*

	Lohkoketjuteknologia	Nykyinen järjestelmä
Transaktioiden verifiointinopeus	X	
Transaktion kustannustehokkuus	X	
Rahan moninkertainen käyttö		X
Kirjanpito	X	
Yksityisyydensuoja	X	
Skaalautuvuus		X
Asiakkaan suoja		X
Sovittelu		X
Transaktion riitauttaminen		X
Järjestelmän energiatehokkuus		X
Mahdollisuus rikollisiin toimiin	X	
Mahdolliset voimakeskittymät		X

LÄHTEET

Abrazhevich, D. Dani, A. Radha, R. Krishna, P. Wang, G. & Das, A. (2001). Classification and Characteristics of Electronic Payment Systems. Electronic Commerce and Web Technologies: Second International Conference, EC-Web 2001. pp. 81 – 100, 122-129.

Bashir, I. (2017). Mastering Blockchain. UK: Packt Publishing.

Bayer, D. Haber, S. Stornetta, W. S. (1993). Improving the efficiency and reliability of digital time-stamping. In Sequences II: Methods in Communication, Security and Computer Science.

Bresnahan, T.F. & Trajtenberg, M. (1995). General purpose technologies Engines of growth. Journal of econometrics, 65(1).

Böhme, R. Christin, N. Edelman, B. & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. The Journal of Economic Perspectives. 29, No.2, pp.213-238.

Chanjaroen, C. and Boey, D. (2016). Fraud in $4 trillion trade finance has banks turning digital. Saatavissa (2.12.2017): http://www.bloomberg.com/news/articles/2016-05-22/fraud-in-4-trillion-trade-finance- turns-banks-to-digital-ledger.

Clayton, M.C. Raynor, M.E. & McDonald, R. (2015). What Is Disruptive Innovation?. Harvard Business Review: December.

Coase, R. H. (1937). The Nature of the Firm. The London School of Economics and Political Science: Economica, 4(16): ss.386–405.

Coleman, J. (1990). Foundations of Social Theory. Harvard University Press,

Dai, W. (1998). b-money. Saatavissa (15.9.2017): http://www.weidai.com/bmoney.txt.

Dandapani, K. (2017). Electronic finance – recent developments, Managerial Finance, Vol. 43(5), pp. 614-626.

Diffie, W. & Hellman, M. E. (1976). New Direction in Cryptography. IEEE Transactions on Information Theory 22(11): 644-54.

Dourado, E., & Brito, J. (2014). Cryptocurrency. The New Palgrave Dictionary of Economics.

Dow, S. & Earl, P. (1982). Money Matters: A Keynesian Approach to Monetary Policy. Oxford: Robertson.

Fanning, K. & Centers, D.P. (2016). Blockchain and Its Coming Impact on Financial Services, Journal of Corporate Accounting & Finance, Vol. 27(5), pp. 53-57.

Ferguson, N. Myers, J. J. (2008). The Ascent of Money: A Financial History of the World. US: Penguin Books.

Franco, P. (2014). Understanding Bitcoin: Cryptography, Engineering and Economics, United Kingdom: Wiley.

Haber, S. & Stornetta, W.S. (1991). How to time-stamp a digital document. In Journal of Cryptology, vol 3, no 2.

Haber, S. & Stornetta, W.S. (1997). Secure Names for Bit-Strings. Nakamoto Institute. Saatavissa (1.12.2017): http://nakamotoinstitute.org/static/docs/secure-names-bit-strings.pdf.

He, D. Habermeier, K. Leckow, R. Haksar, V. Almeida, Y. Kashima, M. Kyriakos-Saad, N. Oura, H. Sedik, T.S. Stetsenko, N. & Verdugo-Yepes, C. (2016). Virtual Currencies and Beyond: Initial Considerations. International Monetary Fund. Saatavissa (26.10.2017): https://www.bitcoinnews.ch/wp-content/uploads/2013/12/sdn1603.pdf.

Jones, S. Wilinkens, M. Morris, P. & Masera, M. (2000). Trust requirements in e-business. COMMUNICATIONS OF THE ACM, Vol 43. No 12.

Knights, D. Noble, F. Vurdubakis, T. & Willmott, H. (2001). Chasing shadows: Control, virtuality and the production of trust. Organization Studies 22/2 311-336. EGOS.

Lipsey, R., Carlaw, K., & Bekhar C. (2005). Economic Transformations: General Purpose Technologies and Long Term Economic Growth. Oxford University Press.

Mainelli, M. & Smith, M. (2015). Sharing Ledgers for Sharing Economies: An Exploration of Mutual Distributed Ledgers (aka Blockchain Technology). Journal of Financial Perspectives, Vol. 3(3), pp. 38-59.

Malinova, K. & Park, A. (2016). Market Design for Trading with Blockchain Technology. Journal of payments strategy & systems, Vol. 9(4).

Massias, H. Avila, X.S. & Quisquater J.J. (1999). Design of a secure timestamping service with minimal trust requirements. In 20th Symposium on Information Theory in the Benelux. Louvain-la-Neuve, Belgium.

Nakamoto S. (2008). Bitcoin: A peer-to-peer electronic cash system. Saatavissa (15.9.2017): https://bitcoin.org/bitcoin.pdf.

Nofer, M. Gomber, P. Hinz, O. & Schiereck, D. (2017). Blockchain. Bus Inf Syst Eng 59(3):183–187 (2017), Springer.

Nokelainen, T. (2011). Lähdeviittauskäytännön periaatteet tieteellisessä kirjoittamisessa. Tampereen teknillinen yliopisto, Tampere, 1-16 p.

O'Mahony, D. Peirce, M. & Tewari, H. (2001). Electronic Payment Systems For E-commerce. 2nd ed. ed. Artech House Inc, Norwood.

Pagano, U., & Vatiero, M. (2014). Costly institutions as substitutes: Novelty and limits of the Coasian approach. Journal of Institutional Economics: University of Siena. 11(2): 265–281.

Panurach, P. (1996). Money in electronic commerce. Communications of the ACM, Vol. 39(6), pp. 45-50.

Pilkington, M. (2016). Blockchain technology: Principles and applications. Research Handbook on Digital Transformations. Edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar, 2016.

Pinna, A. & Ruttenberg, W. (2016). Distributed ledger technologies in securities post-trading. European Central Bank: No 172.

Rochet, J. C. & Tirole, J. (2003). Platform competition in two sided markets. Journal of the European Economic Association, 1(4): 990–1029.

Rogers, E.M. (2003). Diffusion of Innovations, 5th Edition. Free Press, Simon & Schuster New York.

Salam, A.F. Rao, H.R. & Pegels, C.C. (2003). Consumer-perceived risk in e-commerce transactions. Communications of the ACM, Vol. 46(12), pp. 325-331.

Schumpeter, J. A. (1942). Capitalism, Socialism and Democracy. Harper & Brothers.

Tasca, P. Aste, T. Pelizzon, L. Perony, N. (2016). Banking Beyond Banks and Money, 1st ed. 2017 ed. Springer Verlag, DE.

Thierer, A. (2014). Permissionless Innovation: The Continuing Case for Com-prehensive Technological Freedom. Mercatus Center at George Mason Uni-versity.

Wright, A. & De Filippi, P. (2015). Decentralized blockchain technology and the rise of Lex Cryptographia.

Yermack, D. (2017). Corporate Governance and Blockchains, Review of Finance, Vol. 21(1), pp. 7-31.

Yli-Huumo, J. Ko, D. Choi, S., Park, S. & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?. A Systematic Review, PLoS One, Vol. 11(10).

Zacks Equity Research. (2016). Microsoft and BAML to Test Blockchain for Trade Finance. Newstex.